CLAIMS

What is claimed is:

1. A backup server for a wireless subscriber device comprising:

a transceiver for enabling network communication with the wireless subscriber device;

a monitor device, coupled to the transceiver, for monitoring the wireless subscriber device to detect whether a memory of the wireless subscriber device has been compromised; and

a backup memory coupled to the monitor device for storing backup data related to a memory of the wireless subscriber device as determined by the monitor device.

2. The backup server of claim 1, wherein the backup memory is for storing data corresponding to memory changes in the wireless subscriber device as the backup data.

3. The backup server of claim 2, wherein the data corresponding to memory changes comprises one of an original memory state and a log of memory changes at the wireless subscriber device.

4. The backup server of claim 1, wherein the monitor device includes a virus checker for protecting the wireless subscriber device against viruses.

5. The backup server of claim 4, wherein the virus checker is operable for restoration of an original memory state of the wireless subscriber device when the virus checker detects a virus.

6. The backup server of claim 5, wherein the backup memory is further for storing previous uninfected versions of software for replacing corresponding infected versions of the software when necessary.

7. The backup server of claim 4, wherein the monitor device further includes a virus elimination program to eliminate viruses from the wireless subscriber device.

8. The backup server of claim 4, wherein the virus checker is further for monitoring for viruses during network downloads to the wireless subscriber device and for preventing the wireless subscriber device from being infected by the viruses.

9. The backup server of claim 4, wherein the virus checker is further for distributing fixes when a virus infects the wireless subscriber device.

10. The backup server of claim 4, wherein the virus checker is updated with new virus information for use in determining whether the wireless subscriber device has been infected with a virus.

11. The backup server of claim 10 wherein the virus checker, when updated with the new virus information, is used to re-scan the backup data to insure that a new virus is not found in the backup data.

12. The backup server of claim 1, wherein the monitor device is for periodically creating copies of memory images of the wireless subscriber device in the backup memory as the backup data.

13. The backup server of claim 12, wherein the monitor device is for purging the copies of memory images of the wireless subscriber device on a predetermined basis.

14. The backup server of claim 1, wherein the monitor device is for duplicating a memory image of the wireless subscriber device after memory updates at the wireless subscriber device as the backup data.

15. A method for maintaining integrity of a memory of a wireless subscriber device, comprising:

remotely maintaining an archived representation and a current representation of the memory of the wireless subscriber device;

determining whether the memory of the wireless subscriber device has been compromised upon occurrence of one of a virus and a virus alert; and

causing the memory of the wireless subscriber device to be restored with the archived memory representation of the wireless subscriber device if the memory of the wireless subscriber device has been compromised.

16. The method of claim 15 further comprising, monitoring the memory of the wireless subscriber device for virus infection prior to determining whether the memory of the wireless subscriber device has been compromised upon occurrence of one of a virus and a virus alert.

17. The method of claim 15, wherein the remotely maintaining the archived representation and the current representation of the memory of the wireless subscriber device further comprises remotely maintaining a log of changes to the memory of the wireless subscriber device for use in the determining whether the memory of the wireless subscriber device has been compromised upon occurrence of one of a virus and a virus alert.

18. A method for backing up a memory of a wireless subscriber device, comprising:

detecting a request by the wireless subscriber device for a network download;

remotely creating an archived representation of a memory image of the memory; and

remotely creating a modified representation of the memory image of the wireless subscriber device during the network download.

19. The method of claim 18, further comprising:

checking the modified representation of the memory image for corruption; and

restoring the wireless subscriber device with the archived representation of the memory image when the checking the modified representation of the memory image for corruption results in detection of an abnormality.

20. The method of claim 18, further comprising:

checking the modified representation of the memory image for viruses; and

eliminating a virus from the wireless subscriber device when the checking of the modified representation of the memory image for viruses after the network download results in detection of a virus.

21. The method of claim 20, wherein the eliminating a virus from the wireless subscriber device comprises eliminating a virus from the wireless subscriber device by enabling a virus elimination program.

22. The method of claim 20, further comprising

re-checking one of the modified representation and the archived representation of the memory image for viruses whenever new virus information is available and

when a virus is detected, eliminating the virus from the one of the modified representation and the archived representation of the memory image and the wireless subscriber device if it is infected by the virus.

23. The method of claim 18, further comprising:

checking the modified representation of the memory image for viruses during the network download; and

interceding during the network download when the checking of the modified representation of the memory image for viruses during the network download results in detection of a virus.

24. The method of claim 23, wherein the interceding during the network download when the checking of the modified representation of the memory image for viruses during the network download results in detection of a virus comprises one of preventing the network download and eliminating the virus from the network download.